

Contents

1	Introduction	1
1.1	Brief Introduction to Cloud Storage Systems	1
1.1.1	Cloud Computing	1
1.1.2	Cloud Storage as a Service.	2
1.2	Data Security for Cloud Storage Systems	3
1.2.1	Storage Auditing as a Service.	3
1.2.2	Access Control as a Service	4
	References	5
2	TSAS: Third-Party Storage Auditing Service	7
2.1	Introduction	7
2.2	Preliminaries and Definitions	9
2.2.1	Bilinear Pairing.	9
2.2.2	Computational Bilinear Diffie-Hellman Assumption	9
2.2.3	Definition of System Model	10
2.2.4	Definition of Security Model	11
2.3	An Efficient and Privacy-Preserving Auditing Protocol	12
2.3.1	Overview	12
2.3.2	Algorithms for Auditing Protocol	12
2.3.3	Construction of the Privacy-Preserving Auditing Protocol	15
2.3.4	Correctness Proof	16
2.4	Secure Dynamic Auditing.	17
2.4.1	Solution of Dynamic Auditing	18
2.4.2	Algorithms and Constructions for Dynamic Auditing	18
2.5	Batch Auditing for Multi-Owner and Multi-Cloud.	21
2.5.1	Algorithms for Batch Auditing for Multi-Owner and Multi-Cloud	21
2.5.2	Correctness Proof	24
2.6	Security Analysis.	25
2.6.1	Provably Secure Under the Security Model	25
2.6.2	Privacy-Preserving Guarantee.	27
2.6.3	Proof of the Interactive Proof System	27

2.7	Performance Analysis	28
2.7.1	Storage Overhead	29
2.7.2	Communication Cost	30
2.7.3	Computation Complexity	31
2.7.4	Computation Cost of the Owner	32
2.8	Related Work	33
2.9	Conclusion	36
	References	36
3	ABAC: Attribute-Based Access Control	39
3.1	Introduction	39
3.2	Preliminary	40
3.2.1	Access Structures	40
3.2.2	Linear Secret Sharing Schemes	41
3.2.3	Bilinear Pairing	41
3.2.4	q-Parallel BDHE Assumption	42
3.3	System and Security Model	42
3.3.1	System Model	42
3.3.2	Framework	44
3.3.3	Security Model	44
3.4	ABAC: Attribute-Based Access Control with Efficient Revocation	45
3.4.1	Overview	45
3.4.2	Construction of ABAC	46
3.4.3	Attribute Revocation Method	48
3.5	Analysis of ABAC	51
3.5.1	Security Analysis	51
3.5.2	Performance Analysis	52
3.6	Related Work	55
3.7	Conclusion	57
	References	57
4	DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems	59
4.1	Introduction	59
4.2	System Model and Security Model	60
4.2.1	System Model	60
4.2.2	DAC-MACS Framework	62
4.2.3	Security Model	63
4.3	DAC-MACS: Data Access Control for Multi-Authority Cloud Storage	65
4.3.1	Overview	65
4.3.2	Construction of DAC-MACS	66
4.3.3	Efficient Attribute Revocation for DAC-MACS	69

- 4.4 Analysis of DAC-MACS 71
 - 4.4.1 Comprehensive Analysis 72
 - 4.4.2 Security Analysis 72
 - 4.4.3 Performance Analysis 77
- 4.5 Related Work 79
- 4.6 Conclusion 81
- References 82



<http://www.springer.com/978-1-4614-7872-0>

Security for Cloud Storage Systems

Yang, K.; Xiaohua, J.

2014, XI, 83 p. 11 illus., Softcover

ISBN: 978-1-4614-7872-0